11-24-00 A

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1 53(b))

Attorney Docket No.	206314
First Inventor	GASTON
Title	Method and Apparatus for Securely Associating an Optically Readable Memory with a User Machine
Express Mail Label No.	EL643541530US

APPLICATION ELEMENTS

1. ☒ Utility Patent Application Transmittal Form
2. ☒ Applicant claims small entity status. See 37 CFR 1.27.
3. ☒ Specification (including claims and abstract) [Total Pages 25]
4. ☒ Drawings [Total Sheets 6]
5. ☒ Combined Declaration and Power of Attorney [Total Pages 3]
   a. ☒ Newly executed
   b. ☐ Copy from prior application [Note Box 6 below]
      i. ☐ Deletion of Inventor(s) Signed statement attached deleting inventor(s) named in the prior application
6. ☐ Incorporation by Reference: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b is considered as part of the disclosure of the accompanying application and is hereby incorporated by reference
7. ☐ Application Data Sheet. See 37 CFR 1.76
8. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix)
9. Nucleotide and/or Amino Acid Sequence Submission
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper Copy
   c. ☐ Statement verifying identity of above copies

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

ACCOMPANYING APPLICATION PARTS

10. ☐ Applicant requests early publication. (include publication fee under 37 CFR 1.18(d))
11. ☐ Assignment Papers (cover sheet and document(s))
12. ☐ 37 CFR 3.73(b) Statement (when there is an Assignee)
13. ☐ Power of Attorney
14. ☐ English Translation Document (if applicable)
15. ☐ Information Disclosure Statement (IDS)
    ☐ Form PTO-1449
    ☐ Copies of Listed Documents
16. ☐ Preliminary Amendment
17. ☒ Return Receipt Postcard (Should be specifically itemized)
18. ☐ Certified Copy of Priority Document(s)
19. ☐ Request & Certification Under 35 USC 122(b)(2)(B)(i) (Form PTO/SB/35 or its equivalent attached)
20. ☒ Other: Application Cover Sheet
    Verified Statement (Declaration)
    Claiming Small Entity Status

21. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information in (a) and (b) below:

    (a) ☐ Continuation ☐ Divisional ☒ Continuation-in-part of prior application no. 09/190,511. Prior application information: Examiner S. Kabakoff; Group Art Unit: 2132

    (b) Preliminary Amendment: Benefit of earlier filing date - 35 USC 120. The Commissioner is requested to amend the specification by inserting the following sentence before the first line:
    "This is a ☐ continuation ☐ divisional ☐ continuation-in-part (CIP) of
    ☐ Application No. , filed on , which is incorporated by reference."
    ☐ International Application No. , filed on , which designates the U.S., and which is incorporated by reference."

UTILITY PATENT APPLICATION TRANSMITTAL | Attorney Docket No. 206314

APPLICATION FEES				
BASIC FEE				$710.00
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total Claims	34 -20=		x $18.00	$252.00
Independent Claims	2 - 3=		x $80.00	$ 0
☐ Multiple Dependent Claim if applicable			+$270.00	$ 0
			Total of above calculations =	$962.00
			Reduction by 50% for filing by small entity =	$(481.00)
☐ Assignment fee if applicable			+ $40.00	$ 0
☐ Early publication fee if applicable			+ $300.00	$ 0
			TOTAL =	$481.00

22. ☐ Please charge my Deposit Account No. 12-1216 in the amount of $.

23. ☒ A check in the amount of $481.00 is enclosed.

24. The Commissioner is hereby authorized to credit overpayments or charge any additional fees of the following types to Deposit Account No. 12-1216:
    a. ☒ Fees required under 37 CFR 1.16.
    b. ☒ Fees required under 37 CFR 1.17.

25. ☒ The Commissioner is hereby generally authorized under 37 CFR 1.136(a)(3) to treat any future reply in this or any related application filed pursuant to 37 CFR 1.53 requiring an extension of time as incorporating a request therefor, and the Commissioner is hereby specifically authorized to charge Deposit Account No. 12-1216 for any fee that may be due in connection with such a request for an extension of time

26. CORRESPONDENCE ADDRESS

☒Customer Number: 23460 **23460** PATENT TRADEMARK OFFICE	☐Phillip M. Pippenger, Reg. No. 46055 Leydig, Voit & Mayer, Ltd. Two Prudential Plaza, Suite 4900 180 North Stetson Chicago, Illinois 60601-6780 (312) 616-5600 (telephone) (312) 616-5700 (facsimile)

Name	Phillip M. Pippenger, Registration No. 46055
Signature	
Date	November 22, 2000

Certificate of Mailing Under 37 CFR 1.10

I hereby certify that this Utility Patent Application Transmittal and all accompanying documents are being deposited with the United States Postal Service "Express Mail Post Office To Addressee" Service under 37 CFR 1.10 on the date indicated below and is addressed to: Assistant Commissioner of Patents, Box Patent Application, Washington, D.C. 20231.

Renato Melero		November 22, 2000
Name of Person Signing	Signature	Date

Utility (Rev. 11/13/2000)

PATENT
Attorney Docket No. 206314

Applicant or Patentee: Kerry R. Gaston
Appln. or Patent No.:
Filed or Issued:
For: Method and Apparatus for Securely Associating an Optically Readable Memory with a User Machine

VERIFIED STATEMENT (DECLARATION)
CLAIMING SMALL ENTITY STATUS
37 C.F.R. §§ 1.9(f) & 1.27(b) - INDEPENDENT INVENTOR

As a below-named inventor, I hereby declare that I qualify as an independent inventor as defined in 37 C.F.R. § 1.9(c), for purposes of paying reduced fees under Sections 41(a) and (b) of Title 35, United States Code, to the Patent and Trademark Office with regard to the invention entitled:

METHOD AND APPARATUS FOR SECURELY ASSOCIATING AN OPTICALLY READABLE MEMORY WITH A USER MACHINE

described in:

☒ The specification filed herewith.
☐ Application No. , filed .
☐ Patent No. , issued .

Others Having Rights In The Invention

I have not assigned, granted, conveyed, or licensed, and I am not under any obligation under contract or law to assign, grant, convey, or license, any rights in the invention to any person who could not be classified as an independent inventor under 37 C.F.R. § 1.9(c) if that person had made the invention, or to any concern which would not qualify as a small business concern under 37 C.F.R. § 1.9(d) or a nonprofit organization under 37 C.F.R. § 1.9(e).

Each person, concern, or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

☒ no such person, concern, or organization.
☐ persons, concerns, or organizations listed below. (NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to his/her/its status as a small entity.)

Name:
Address:

☐ Individual ☐ Small Business Concern ☐ Nonprofit Organization

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 C.F.R. § 1.28(b)).

I hereby declare that all statements made herein of my own knowledge are true, that all statements made on information and belief are believed to be true, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

Name of Inventor: Kerry R. Gaston

Signature of Inventor

November 16, 2000
Date

gaston\app\206314 SES

Attorney Docket No.
206314

PATENT APPLICATION

Invention Title:

METHOD AND APPARATUS FOR SECURELY ASSOCIATING AN OPTICALLY READABLE MEMORY WITH A USER MACHINE

Inventors:

Kerry R. Gaston	U.S.A.	Montgomery	AL
INVENTOR'S NAME	CITIZENSHIP	CITY OF RESIDENCE	STATE or FOREIGN COUNTRY

Be it known that the inventors listed above have invented a certain new and useful invention with the title shown above of which the following is a specification.

METHOD AND APPARATUS FOR SECURELY ASSOCIATING AN OPTICALLY READABLE MEMORY WITH A USER MACHINE

Related Applications

This application is a continuation in part of co-pending United States Patent Application serial number 09/190,511, filed on November 12, 1998, entitled "Secure Optically Readable Memory Usable In Conjunction With a Limited Number of Machines," which is hereby incorporated by reference in its entirety.

Field of the Invention

The present invention relates generally to the field of optically readable memory, and more particularly, relates to an optically readable memory that can be made secure and usable in connection with a limited number of machines.

Background of the Invention

CD-ROM discs are capable of storing large quantities of digital information. This information may be program, database, image, music, video, desktop publishing, or other information susceptible to digital storage. The information is generally stored by physical pits and lands situated along a spiral track that is several miles long. The physical pits may be made optically or by direct physical manipulation, but are readable only optically. That a memory is optically readable means herein that the memory is readable through the use of a laser or other light source.

There are generally two alternate methods that may be used to manufacture CD-ROM's with specific information on them. The first of these is "glass mastering", which begins with creation of a first copy of the disc which will be used to create a series of positive and negative copies, which will then be used to press identical copies of the first disc. This method, with possibly only a few exceptions, does not allow for the placement

of unique information on any one copy. "CD-R" is an alternative writing process, wherein a layer of organic dye allows the CD-R disc to have a unique set of data recorded on it by a CD-R recorder. Copies made by the CD-R method need not be identical. Rather, each may contain certain unique information. Whichever method is used, each copy of the disc is generally coated with a reflective coating and a clear protective layer after being encoded with information.

In FIG. 1, there is shown a sectional side view of a prior art disc, taken along a radius of the disc. The data on the disc is represented by the structure **2** imprinted on the disc. As mentioned, the structure **2** representing the data is generally covered by a clear protective coating **4**, after being covered by a thin reflective layer which is not depicted in the figures for simplicity. Generally, the information stored on a CD-ROM is read by directing a low-power laser (typically solid-state or HeNe) at the portion of the spiral track containing the information to be read, along the direction **6**. Because the pits reflect light differently than the plains or lands between pits, a photodiode or other photosensitive receiver **8** exposed to the reflected light will detect a series of light and dark reflections as the disc spins, which can be converted to a series of 1's and 0's. These 1's and 0's are a digital representation of the information stored on the disc. Generally, to ensure that the pits and lands pass the laser and receptor **8** at the same rate regardless of location, the disc turns at a lower angular velocity as sectors farther from the center are read.

As a high-density storage medium, CD-ROM technology involves the use of channel codes to retrieve the information stored on the disc. Typically, the channel code used is eight-to-fourteen modulation, a method that relies on transitions to signal ones, and the absence of transitions to signal zeros. Because of this high density and resulting high storage capacity, CD-ROM technology has emerged as a superior alternative to floppy disc technology for marketing large application programs or other memory intensive data. Furthermore, the fact that they are an optical rather than magnetic

medium makes CD-ROM's impervious to influences that would corrupt a floppy disc. Even the laser that is typically used by a user machine to read a CD-ROM disc is incapable of damaging or writing on the disc. Hence the moniker, ROM or Read Only Memory.

In the past, the inability of user machines to write on CD-ROM's has caused CD-ROM's to be difficult to secure. Once one user had acquired a disc, there was no way to avoid the dissemination of the information on the disc to other users. In light of this problem with CD-ROM's, certain security measures have developed. In one prior art scheme, a CD-ROM is packaged with a companion floppy disc, which is magnetically readable and writeable by the user computer, to be used along with the CD-ROM to access the information on the CD-ROM. The floppy, which contains information necessary to the use of the CD, is copy-protected. However, the security provided by this scheme is compromised by the widespread availability of means to defeat copy protection on floppy discs.

Methods of copy-protecting a CD itself include the method and apparatus claimed by Kikinis as disclosed in U.S. Patent Number 5,596,639. The invention of Kikinis involves the use of a high-powered laser to damage the physical structure of the disc, in selected areas, to create a password. Drawbacks to this method are readily apparent; the programming of the password onto the disc requires a higher power laser than that used by the user computer. Thus there is no way, using this method, for the information on the disc to indicate whether the disc has been used already. Consequently, although the disc may be copy-protected, it is not protected from use by more than one user computer.

To overcome the drawbacks evident in the prior art, it is desirable to provide an optically readable memory that prevents unauthorized use. For example, it is desirable to provide a CD-ROM that is capable of changing in response to an authorized use in order to block subsequent unauthorized use. To this end, according to an embodiment, the optically readable memory of the present invention is adapted to be permanently altered

by a finite number of read cycles, so that a vanishing code located on the disc, usable to access the disc, becomes unreadable. Alternatively, in an embodiment of the invention, the user machine may alter the optically readable memory by writing rather than obscuring security information.

Summary of the Invention

An object of the present invention is to provide an optically readable memory that is usable in connection with a finite number of user machines. Generally, this object is achieved by providing the optically readable memory with a vanishing code, usable to access information stored on the memory. The vanishing code is digitally written on the optically readable memory and is situated physically adjacent or proximal to an initially translucent mask layer. The mask layer is adapted to cause the vanishing code to become unreadable after at least one and possibly multiple readings by a user machine. In this manner, a user machine that has not already read the vanishing code will be unable to access the information stored on the disc after the vanishing code becomes unreadable.

In an alternative embodiment, a signature is created by manipulating numerical indicators that may be predominantly unique to a user machine. Thereafter, the signature is written to the disc, preventing later access to secured information on the disc via any machine other than a machine which has unique information that yields essentially the same signature initially written to the disc. A distinct aspect of this embodiment is to provide a CD-ROM that is writable using a standard CD-ROM read laser.

The optically readable memory is preferably a CD-ROM, and the mask layer is preferably sensitive to low-power laser radiation such as that emitted by a solid-state or HeNe laser of the wavelength typically used by a user machine to read CD-ROM's. The mask layer is preferably a thin film or substrate positioned on the CD-ROM above the pits and lands representative of the vanishing code, but beneath the standard clear

protective layer. In one embodiment, the mask layer preferably becomes permanently altered to render the vanishing code unreadable after a finite number of exposures to the radiation used to read the disc, while in another embodiment, the mask layer may be selectively altered to provide a readable data encoding function.

Brief Description of the Drawings

FIG. 1 is a fragmentary sectional side view of a prior art disc, taken along a radius of the disc;

FIG. 2 is a fragmentary sectional side view of a vanishing code portion of a disc according to an embodiment of the present invention, taken along a radius of the disc, wherein the disc has not yet been read by a user machine;

FIG. 3 is a fragmentary sectional side view of the vanishing code portion of a disc according to an embodiment of the present invention, taken along a radius of the disc, wherein the disc has been previously read by a user machine;

FIG. 4 is a flow chart representing the process used to grant or deny access to the information stored on a CD-ROM in an embodiment of the present invention;

FIG. 5a is a simplified sectional side view of the obscurable section of a disc according to an embodiment of the present invention, taken along a radius of the disc, wherein the disc has not yet been read by a user machine;

FIG. 5b is a sectional side view of the obscurable section of a disc according to an embodiment of the present invention, taken along a radius of the disc, wherein the disc has been previously read by a user machine;

FIG. 5c is a sectional side view of the obscurable section of a disc according to another embodiment of the present invention, taken along a radius of the disc, wherein the disc has been previously read by a user machine;

FIG. 6 depicts a flow chart representing the process used to grant or deny access to the information stored on a CD-ROM in an alternative embodiment of the present invention;

FIG. 7 is a schematic illustration of an exemplary system in which the memory of the present invention may be used; and

FIG. 8 is a sectional side view of a disc according to an embodiment of the present invention, taken along a radius of the disc.

Detailed Description of the Preferred Embodiments

Turning to the figures, wherein like numerals designate like parts, there is shown in FIG. 2 a cross-sectional view of the vanishing code portion of a CD-ROM according to an embodiment of the invention, prior to use. In particular, the CD-ROM includes structure which represents digital data corresponding to a vanishing code **10**, a standard clear protective coating **12**, and a mask layer **14** disposed beneath the clear protective coating **12**. The mask layer **14** may cover the entire vanishing code, or may cover only a portion of the vanishing code. The structure that represents the information and data on the disc may be disposed along a spiral track on the disc, as in the prior art. The vanishing code may be unique to the disc or, preferably, it may be the same for all copies of the same-titled CD-ROM. The laser radiation employed by the user machine's CD-ROM drive to read the disc is directed along line **16**. During scanning of the vanishing code region, the laser radiation is transmitted through both the clear protective coating **12** and the mask layer **14**, which is transparent prior to use. Upon striking a pit **18**, the laser radiation reflects differently than upon striking a land **20**. A photodiode or other photosensitive receiver **22** situated to receive reflected or transmitted laser radiation detects the relative strength of reflected or transmitted light. Upon further processing, the detected series of strong and weak reflections or transmissions is converted to a digital series of 1's and 0's, representing the vanishing code. In this manner, the user machine

may read and store the vanishing code when first presented with a new disc embodying the present invention. As will be described hereinafter, the vanishing code is preferably usable by the user machine to access the information stored on the CD-ROM. Possibly, the vanishing code is used in conjunction with a hidden code, much as a key is used in conjunction with a lock, to gain access to whatever application or data is stored on the CD-ROM.

The mask layer **14** will now be described in greater detail. The mask layer **14** is depicted and described in an exemplary embodiment as a distinct coating, but may in fact alternatively be an integral part of another layer of the disc pursuant to certain fabrication methods. As will be described, the mask material may darken or become opaque due to photoreaction, or alternatively may change from non-reflective to reflective upon photoreaction. Generally, methods of fabricating the mask layer **14** can be divided into two categories: surface deposition and integral doping/implantation (such as ion implantation). Surface deposition techniques include sputtering, physical or chemical vapor deposition, spin coating, rear-side ablation of organic chromophore, and pulsed laser evaporation. Note that the surface upon which the mask layer is deposited may be the pitted information surface of the disc, or may be the opposite side, or "smooth" side, of the disc, or the reflective layer itself.

Appropriate doping/implantation methods include ion implantation into the typically polycarbonate substrate, either before or after processing, or into the reflective coating or other component, and doping of the disc feedstock used for forming the disc. Doping/implantation methods may be used to alter any of the disc constituent layers, including the substrate and the reflective layer.

Materials suitable for masking via deposition or doping/implantation include photoblendable metal compounds and photodarkenable amorphous compound semiconductor thin films or particles. As one example of a depositable photoreactive coating, a quantum-dot loaded liquid polymer may be spun onto the desired surface of the

disc. In an exemplary integral technique, as an alternative to placing photodarkening compounds into the reflective layer, oxygen compounds which are sensitive to light may be placed in the reflective layer, which is typically aluminum. In this way, laser radiation that is incident upon the aluminum will act to release oxygen into the aluminum, causing it to become substantially non-reflective to the laser radiation.

One suitable technique that requires additional processing steps involves the use of ultraviolet conditioning for infrared absorption. In this technique, a light-sensitive coating or constituent (UV chromophores may be deposited on any surface of the disc by way of spin coating, or may be doped or implanted into the disc) is incubated via UV (high-energy) radiation prior to use, such as during manufacture, such that later exposure to infrared (low-energy) radiation activates the material, causing a change in the optical properties of the material. Because the material resides either proximally to or within a layer of the disc, the change in optical properties alters the reflection or transmission of incident read laser radiation. The technique of ultraviolet conditioning for infrared absorption has the benefit of allowing indiscriminate placement of a fairly photo-insensitive mask layer, either within or on a disc constituent, over a large portion of the disc, followed by selective incubation to sensitize only those portions of the disc (the obscurable section) where information is desired to be later written or obscured. Thus, an acceptably small reaction time constant may be selectively provided within the obscurable section without risking inadvertent photodarkening through routine reads of the disc outside of the obscurable section.

Other photodarkenable materials sensitive to infrared (IR) radiation such as that typically used to read CD-ROMs (approximately 780 nm) include silver compounds and chemicals, such as silver soap emulsions, mixtures and solutions. For example, silver soap is the primary ingredient in certain photosensitive films such as DRYVIEW x-ray film produced by KODAK.

FIG. 3 illustrates a cross-sectional view of the vanishing code portion of a CD-ROM according to an embodiment of the invention, after a finite number of scans by the reading laser of the user machine CD-ROM drive. Unlike the mask layer **14** in FIG. 2, the mask layer **14'** in FIG. 3 is opaque. This is due to the light-sensitive nature of the mask layer material, which is particularly adapted in this embodiment to become opaque in response to a finite amount of exposure to infrared radiation, the wavelength range of light typically used to read CD-ROM's. When the user machine attempts to read the vanishing code of the CD-ROM in FIG. 3, which code has become obscured by the now opaque mask layer **14'**, the laser radiation **16'** used by the CD-ROM drive of the user machine does not reflect strongly from, or transmit strongly through, the structure **10'** which represents the vanishing code. Thus, the vanishing code becomes unreadable, and the information stored in the vanishing code region of the CD-ROM is preferably interpreted as an invalid code. As will be described, a user machine which has not acquired the vanishing code before it has become unreadable will preferably not be able to access the data stored on the CD-ROM of FIG. 3.

Alternatively, the mask layer **14'** material may change from non-reflective to reflective upon repeated exposure to optical radiation. In this case, when the user machine attempts to read the vanishing code of the CD-ROM in FIG. 3, which code has become obscured by the now reflective mask layer **14'**, the laser radiation **16'** used by the CD-ROM drive of the user machine reflects from the vanishing code region of the CD-ROM. Thus, the vanishing code becomes unreadable, and the information stored in the vanishing code region of the CD-ROM is preferably interpreted as an invalid code.

There is shown in FIG. 4 a flowchart of the method according to a preferred embodiment whereby the user machine gains, or is denied, access to the information stored on an optically readable memory. At event **100**, the CD-ROM is inserted into the drive of a computer. If the computer has previously used this type of disc, it will have loaded the gatekeeper program from the CD-ROM onto its hard drive. This is because

the CD-ROM causes a computer that does not have the gatekeeper program on its hard drive to have the gatekeeper program installed. Thus, if there is no gatekeeper program on the hard drive, then the computer is instructed to load the freely accessible gatekeeper program onto its hard drive from the CD-ROM at event **104**.

Once the gatekeeper program is installed and running, it functions to locate the vanishing code region of the CD-ROM and attempts to read the code, event **118**. If the code is unreadable, then the gatekeeper program denies the computer access to the encrypted information on the CD-ROM, event **106**. If the code is readable, the computer reads and stores it, using it thereafter to gain access to the encrypted information on the CD-ROM, event **108**. As described previously, the process of reading the code will render the code unreadable after a finite number of scans by the user machine laser.

If the machine has previously been exposed to this type of disc as evidenced by the initial presence of the gatekeeper program on the hard drive, then the machine, using the gatekeeper program, locates the hidden code on the CD-ROM and compares it to vanishing codes that have previously been stored on the hard drive, event **102**. If a match is found, the computer is granted access to the encrypted information on the disc, event **110**. If a match is not found, the computer attempts to read the vanishing code, event **112**. If the code is not readable, access is denied, event **116**. If the code is readable, the computer reads it, permanently stores it in a location used for other codes usable in conjunction with this type of disc, and uses it to access the encrypted information on the disc, event **114**. The process of reading the code will render it unreadable after at least one read.

It may often be useful to use the same hidden and vanishing codes for all copies of the same titled disc. In this manner, a user who has previously bought a copy of that disc and used it in their user machine may also use any other copy of the same disc. This would be true even where the other copy has previously been used by another machine

rendering the vanishing code unreadable, because the user machine seeking access has already stored the hidden code during use of the first copy of the same titled disc.

In an alternative embodiment, the photosensitivity of regions of the disc is exploited to provide security by encoding rather than obscuring information. For example, with reference to FIG. 5, an entirely reflective portion of the disc 300, 300' may incorporate a photodarkenable component, as in FIG. 5c, or be covered by a photodarkenable material 302, 302' as in FIGS. 5a and 5b. (This region will be referred to as an "obscurable section"). The photodarkenable material or component is a material which reacts to radiation of the wavelength used to read the disc, such as the quantum dot, amorphous semiconductor, silver soap and other materials discussed above. In this embodiment, the active concentration or other parameter of the material or component are such that the time constant for optical reaction is significantly increased over that for the previously described embodiment. Accordingly, while routine reads of the relevant area will not quickly induce a darkening or other reaction, sustained exposure to infrared radiation will cause an optical change in the irradiated region, shown by regions 304 and 304' in FIGS. 5b and 5c respectively. Thus, a particular area is altered by directing the read laser at the area for a prolonged period, typically two seconds or less, depending upon the exact parameters of the chosen photodarkenable material or component.

The exposure time to induce an optical change is preferably longer than the cumulative exposure via routine reads over the expected lifetime of the product, to avoid the alteration of encoded data by repeated reading. This said, short exposure times, such as those experienced during a read, are not necessarily strictly cumulative, due to the absence of significant heat build-up and other effects associated with longer exposure times. Thus, for example, if one second of exposure is required to produce an optical alteration, it does not necessarily follow that 1000 separate one-millisecond read exposures will likewise produce the alteration. Rather, significantly more reads would generally be required to produce such an alteration depending upon the material chosen.

Radiation 306 emanating from the read laser is shown for illustration purposes as impinging the disc from both directions. Typically, however, the read laser radiation will initially strike the disc from only one direction, which depends upon the system and disc design. Although this embodiment is described with reference to a photodarkenable mask material, other mask materials, such as non-reflective mask materials that are photoreactive to become reflective, may also be used.

A pattern of such optically altered regions is used in this embodiment to encode information onto the disc, in that for example altered areas may be read as a "1" while unaltered areas in the region are registered as "0," or transitions between altered and unaltered areas within the obscurable section may be read as data. Thus, the disc is writable using the same radiation ordinarily used to read the information on the disc. The particular area of the disc that is written using this method may be as small as a pit or plane, or as larger as, or larger than, a sector or ring of the disc.

A disc according to an embodiment of the invention is produced without having a password or hidden code information encoded thereon, but having thereon a gatekeeper program and an obscurable section as described above. The security function provided by such a disc in this embodiment of the invention is shown in FIG. 6. While the system is described with reference to a CD-ROM and CD-ROM drive, it will be understood by those of skill in the art that the described mechanisms and techniques are more widely applicable to other optical storage media as well. Initially at event 400, the CD-ROM is placed into the CD-ROM drive. In step 402, the gatekeeper program resident on the disc is executed virtually from the CD-ROM.

The gatekeeper program may alternatively be loaded onto a computer or other device and run thereon. In step 404, a gatekeeper verification program, which may be a subpart of the gatekeeper program, is run to confirm, in a manner well-known to those of skill in the art, that the disc is neither faulty nor being hacked. At decision 406, if the disc is determined by the verification program to be unacceptable to run, then in step 408,

the gatekeeper verification program may optionally be repeated one or more times. If the disc remains unacceptable, then at decision 410 the gatekeeper verification program informs the user that the disc is unacceptable in step 412, and may present an explanation of the detected fault or problem as well as a phone number, email address, Internet address, etc. for inquiries and/or ordering information.

Continuing with reference to FIG. 6, if at decision 410, or at decision 406, the disc is determined to be acceptable, then the gatekeeper program locates user unique information ("UUI") in step 414. This information is gathered from the user machine itself, possibly including such information as chip and/or component serial numbers, resident program serial numbers or identifiers, etc. Any information that is detectable and that can be used to attempt to uniquely identify the machine, either alone or in combination with other information is UUI that may be used to create a user machine "signature," which may the UUI itself or a value derived therefrom. For example, one or more chip serial numbers may be gathered and combined or concatenated in a manner to produce a password or code, the signature, that is unlikely to be reproduced for a different machine. The length of the signature produced should be chosen to be writable on the disc using the space allotted within a reasonable amount of time using the particular encoding method and material chosen.

In decision 416, the gatekeeper program locates the obscurable section and determines whether it is clear, i.e. whether or not it has been written to. If the obscurable section is clear, then in step 418, the gatekeeper program writes the signature to the section as described above, as shown in FIG. 6. There are many different ways in which the signature can be written to the obscurable section, depending in part on the size and composition of the obscurable section; for example, the obscurable section may comprise a large or small portion of the disc area, and may be contiguous or fragmented. If the signature is to be written on the level of pits and plains, then the signature may comprise a substantial amount of data, such as a simple listing of chip identities and serial numbers.

If, on the other hand, the granularity of writing is to be less, so that writing occurs on the level of a disc sector or ring, the signature will generally comprise a lesser amount of data. For example, one thousand separate sectors could represent one thousand different signature conditions. Sector 5648 could then be obscured to represent a signature of 5648, and so on, according to the particular algorithm chosen to encode the signature.

More efficiently, each obscured sector or ring from a select group of such (i.e., the obscurable section), can be used to encode a binary digit, so that all or some of the select group could be written to encode a binary string. Using this method, a thousand-condition signature is writable in an obscurable section having only ten writable units, be they sectors or rings. This method, while more efficient in its use of disc space, exacts a greater cost in terms of writing time. One benefit to writing user machine unique information on the disc itself, as opposed to storing disc unique information on the user machine, is that if the user machine loses its stored information, such as through a hard drive crash or otherwise, the machine, once recovered, can still use a disc which had previously been signed using that machine's UUI.

Subsequently in step 420 of FIG. 6, the gatekeeper program runs again, approving the disc for use, and grants the machine access to the protected disc contents, such as by installing the title program from the disc to the user machine.

If at decision 416 it is determined that the obscurable section is not clear, i.e. that it has been written, then in decision 422 the gatekeeper program reads the signature from the obscurable section (the "existing signature") and compares it to a signature derived from the UUI collected in step 412 (the "generated signature"). Since the gatekeeper uses the same algorithm, whether it is writing a signature or just checking a previously written signature, then the existing signature and generated signature will match if the user machine is the same one that wrote the existing signature to the obscurable section. Thus, if the signatures match, then in step 420, the gatekeeper runs the verification program again and approves the disc for use. If however, the signatures are determined at

decision 422 to not match, then in step 424, the gatekeeper may recheck the signatures before disapproving the disc for use and optionally presenting a screen of options as in step 412.

It may be desirable to provide a conditional signature. For example, the signature may consist of a listing of twelve serial numbers, and a match may be found when at least eight of the twelve match. Thus, using such a signature and condition, a user could replace several components of his computer and still have a user machine signature that allows usage of a previously used signed disc of the type described above.

In order to best utilize a signaturized disc as described above, it will in some cases be necessary to enhance the disc drive read protocol as well. In general, large areas of a CD-ROM that contain no data, such as an unwritten obscurable section, may be detected as an "error" by some CD-ROM drives. Accordingly, it is desirable to configure the CD-ROM read protocol to designate such areas, when detected in the region of the obscurable section, as a series of zeroes, for example. Alternatively, certain CD-ROM drives will detect certain disc regions as all zeroes regardless of the content of those areas. Accordingly, if the obscurable section is to be in such an area, then it is desirable to alter the read protocol to detect any change in such an area as a "1."

In one embodiment, the information protected on the CD-ROM is text information, such as the text of a novel, treatise, or periodical. In this embodiment, the CD-ROM is adapted to be used in a device that can read the information and display it or otherwise convey it to the user, once access to the disc is granted. FIG. 7 depicts a variation of this embodiment in which the device **200** which reads the CD-ROM may be physically separate from the means **210** for displaying or otherwise conveying the information read. In this variation, necessary information could be exchanged between the reading means and displaying or conveying means by way of permanent or temporary hardwire, optical, radio transmission, or other means **220**. Such information may be, for example, display, control, or formatting information.

In another preferred embodiment, the gatekeeper program is the same regardless of the contents of the disc.

In a further embodiment, the writing mechanism described above for signaturizing a CD-ROM may be used more generally to place other kinds of information onto the disc via the read laser. For example, a user's program settings or options could be written onto a non-secure disc containing the program so that the user does not have to repeat the information upon using the disc on a different machine. Those of skill in the art will appreciate that any other type of information could be written to the disc in this manner as well. In this embodiment, the obscurable section may, but need not, comprise a large portion of the entire usable data area of the disc.

An alternative embodiment of a suitable disc structure is illustrated schematically in Fig. 8. In particular, the disc 500 is originally processed in a largely conventional manner, with the exception that an outer ring 502 of the disc 500 is protected so that aluminum 504 and lacquer 506 are not initially deposited in the protected region 502. Subsequently, a photoreactive mask layer 508 is deposited on the protected ring 502, followed by a deposition of aluminum 510 or other reflectant, and the application of a protective lacquer 512. In this embodiment, because the mask layer 508 does not cover any part of the disc 500 other than the obscurable section, it need not be initially clear. For example, the mask layer 508 may actually comprise an initially opaque or reflective material which is photoreactive to become reflective or non-reflective respectively. In such a case, there need not be a separate reflective layer 510 adjacent the mask layer.

Deposition of the disc layers within the protected ring 502 may be by way of a reverse masking process, or may alternatively be by way of spin coating such that centrifugal force limits deposition to an outer portion. It may be desirable to use a combination of these techniques by themselves, or in conjunction with other coating techniques. The width of the protected region 502 in this embodiment is preferably

approximately 0.125 inches, but may be much less or much greater than that depending upon a user's preference or constraints.

While the invention has been described with reference to certain exemplary embodiments, there is no intent to limit it to those embodiments. To the contrary, it is recognized that various changes and modifications to the specifically described embodiments will be apparent to those skilled in the art, and that such changes may be made without departing from the spirit and scope of the invention.

For example, the photosensitive mask layer or constituent material may react indirectly to the heat caused by laser radiation rather than directly to the photons or light energy itself. A layer of the disc itself, rather than a mask layer, may be altered by the read laser radiation, energy, or heat. As well, the invention may be embodied in optically readable memory technology other than CD-ROM's. Examples of such other technology include the digital video disc (DVD), Laser Disc, CD-R, and minidisc, and there will likely be developed other optically readable memory systems with which the present invention could be used. It is also recognized that the embodiments of the invention may be used with optical memory technology that operates by transmittance rather than reflectance. It is not critical which side of the disc the mask layer is located upon, as this may be determined in part by the direction from which the optical radiation impinges upon the disc, or the disc manufacturing steps used. Thus, the read laser radiation may or may not pass through the disc substrate depending upon whether the disc is read by transmission or reflection, and in the case of reflection, whether the read laser radiation impinges from the information side or otherwise.

Further, there may be more than one vanishing code on a memory, or a vanishing code may be dispersed piecemeal at different locations on the memory. It is also within the scope of an embodiment of this invention to use a mask layer whose time-constant properties allow reading by a number of machines greater than one before the vanishing code becomes unreadable.

One of skill in the art will appreciate that although the user unique information described in an embodiment of the invention is derived from serial numbers and other numerically stored indicators, it may also be derived from a machine-unique measured value, such as wavelength or power factors of the read laser and so on.

Accordingly, such changes, modifications, and equivalents are intended to be covered by the appended claims and equivalents thereof.

WHAT IS CLAIMED IS:

1. A method of securely providing user information to a user machine adapted to operate in conjunction with an optically readable memory containing information which comprises at least the user information and a gatekeeper program, and having thereon an obscurable section comprising a photoreactive mask layer disposed to alter the detected optical properties of areas of the memory exposed substantially to a wavelength of optical radiation usable to read the memory, the method comprising the steps of:

collecting machine-unique information from the user machine;

generating a user machine signature based on the machine-unique information;

causing the user machine to scan the obscurable section of the memory;

determining whether an existing signature is present in the obscurable section; and

if no existing signature is present in the obscurable section, causing the generated user machine signature to be written in the obscurable section by selectively irradiating the obscurable section with light of the same wavelength used to read the memory, thereby selectively altering the detected optical properties of the memory in the obscurable section, and providing the user information to the user machine; and

if an existing signature is present in the obscurable section, causing the user machine to compare the existing signature to the generated signature, and providing the user information to the user machine if the existing signature matches the generated signature, and denying the user machine access to the user information if the existing signature does not match the generated signature.

2. The method according to claim 1, wherein the step of collecting machine-unique information from the user machine is performed by the gatekeeper program.

3. The method according to claim 1, wherein the machine-unique information includes component-identifying information corresponding to at least one hardware component residing in the user machine.

4. The method according to claim 3, wherein the machine-unique information includes component-identifying information corresponding to a plurality of hardware components residing in the user machine, and wherein the step of comparing the existing signature to the generated signature includes the step of finding a match if a subset of the component-identifying information used to derive the generated signature matches a subset of the component-identifying information used to derive the existing signature.

5. The method according to claim 1, wherein the photoreactive mask layer includes UV chromophores pre-exposed to UV radiation, such that the photoreactive mask layer is sensitized to IR radiation of the wavelength used to read the memory.

6. The method according to claim 5, wherein the UV chromophores are disposed on a surface of the optically readable memory.

7. The method according to claim 5, wherein the UV chromophores are disposed within a layer of the optically readable memory.

8. The method according to claim 1, wherein the photoreactive mask layer includes silver soap.

9. The method according to claim 8, wherein the silver soap is disposed on the surface of the optically readable memory.

10. The method according to claim 8, wherein the silver soap is disposed within a layer of the optically readable memory.

11. The method according to claim 1, wherein the photoreactive mask layer includes amorphous compound semiconductor material.

12. The method according to claim 11, wherein the amorphous compound semiconductor material is disposed on the surface of the optically readable memory.

13. The method according to claim 11, wherein the amorphous compound semiconductor material is disposed within a layer of the optically readable memory.

14. The method according to claim 1, wherein the photoreactive mask layer includes oxygen bearing material disposed within a reflective layer of the memory, adapted to release oxygen into the material of the reflective layer upon encountering IR radiation.

15. The method according to claim 1, wherein the step of causing the generated user machine signature to be written in the obscurable section by selectively irradiating the obscurable section further comprises the step of irradiating the obscurable section with a resolution of individual lands and pits to encode the user machine signature.

16. The method according to claim 1, wherein the step of causing the generated user machine signature to be written in the obscurable section by selectively irradiating the obscurable section further comprises the step of irradiating an individual ring of the optical memory to encode the user machine signature.

17. The method according to claim 16, wherein the step of irradiating an individual ring of the optical memory to encode the user machine signature comprises the step of irradiating a subset of a plurality of rings within the obscurable section to encode a binary representation of the signature.

18. The method according to claim 1, wherein the step of causing the generated user machine signature to be written in the obscurable section by selectively irradiating the obscurable section further comprises the step of irradiating individual sectors of the optical memory to encode the user machine signature.

19. The method according to claim 1, wherein the obscurable section consists of a ring along an outer circumference of the disc surface, and wherein the photoreactive mask layer is disposed only in the obscurable section.

20. The method according to claim 1, wherein the altered detected optical properties of the memory in the obscurable section exhibit a change in the reflectivity of the mask layer.

21. The method according to claim 1, wherein the altered detected optical properties of the memory in the obscurable section exhibit a change in the translucence of the mask layer.

22. An optically readable memory comprising:

at least one obscurable section comprising a photoreactive component,

wherein the photoreactive component is adapted to react to selectively applied optical radiation of the wavelength and power used to read the memory, to digitally encode binary data.

23. The optically readable memory according to claim 22, wherein the photoreactive component includes UV chromophores disposed on a surface of the memory.

24. The optically readable memory according to claim 23, wherein the UV chromophores have been incubated by UV radiation rendering them photosensitive to IR radiation.

25. The optically readable memory according to claim 22, wherein the photoreactive component includes UV chromophores disposed within a layer of the memory.

26. The optically readable memory according to claim 25, wherein the UV chromophores have been incubated by UV radiation rendering them photosensitive to IR radiation.

27. The optically readable memory according to claim 22, wherein the photoreactive component includes silver soap disposed on a surface of the memory.

28. The optically readable memory according to claim 22, wherein the photoreactive component includes silver soap disposed within a layer component of the memory.

29. The optically readable memory according to claim 22, wherein the photoreactive component includes amorphous compound semiconductor material disposed on a surface of the memory.

30. The optically readable memory according to claim 22, wherein the photoreactive component includes amorphous compound semiconductor material disposed within a layer of the memory.

31. The optically readable memory according to claim 22, wherein the photoreactive component includes oxygen bearing material disposed within a reflective layer of the memory, adapted to release oxygen into the material of the reflective layer upon encountering IR radiation.

32. The method according to claim 22, wherein the obscurable section consists of a ring along an outer circumference of the disc surface, and wherein the photoreactive component is disposed only in the obscurable section.

33. The method according to claim 22, wherein the photoreactive component is adapted to exhibit a change in reflectivity upon irradiation by electromagnetic energy of a wavelength used to read the memory.

34. The method according to claim 22, wherein the photoreactive component is adapted to exhibit a change in translucence upon irradiation by electromagnetic energy of a wavelength used to read the memory.

Abstract of the Disclosure

A CD-ROM has an obscurable section wherein exists a photosensitive mask material layer or constituent operative to alter the optical properties of areas subjected to prolonged exposure to the CD-ROM read laser radiation. Digital information stored on a CD-ROM is made accessible by use of a password, which is generated from user machine unique information, and which is written on the CD-ROM via selective exposure of the CD-ROM to the radiation used to read the CD-ROM.

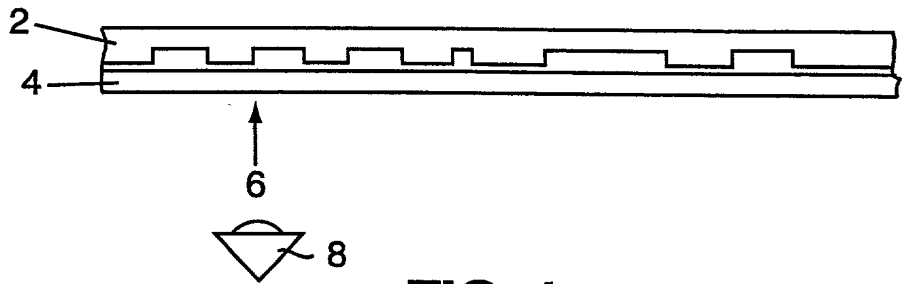


FIG. 1 (Prior Art)

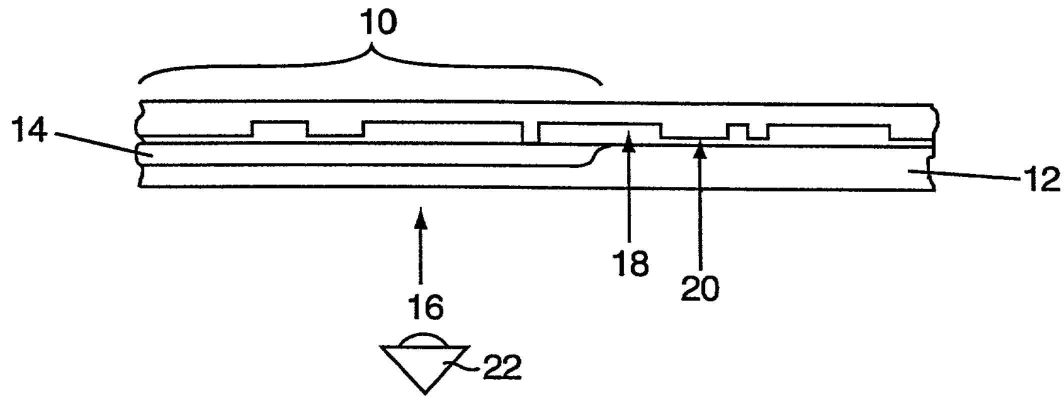


FIG. 2

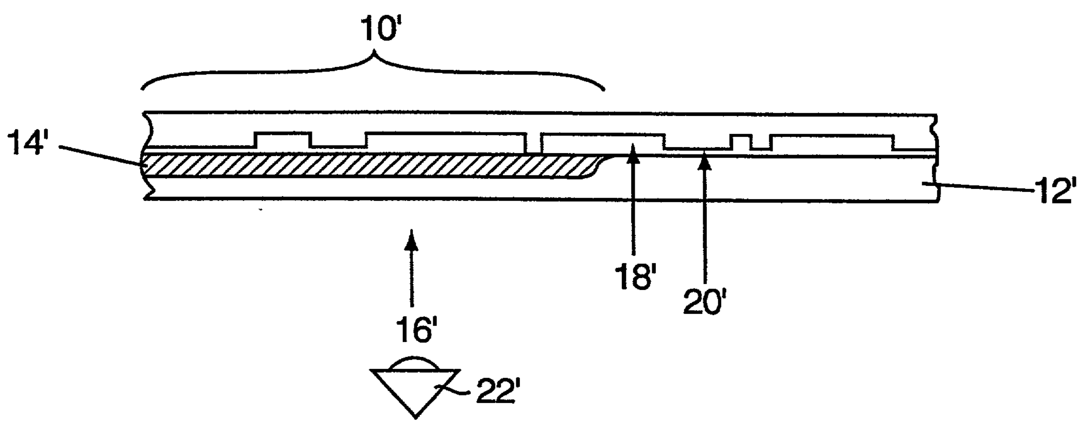
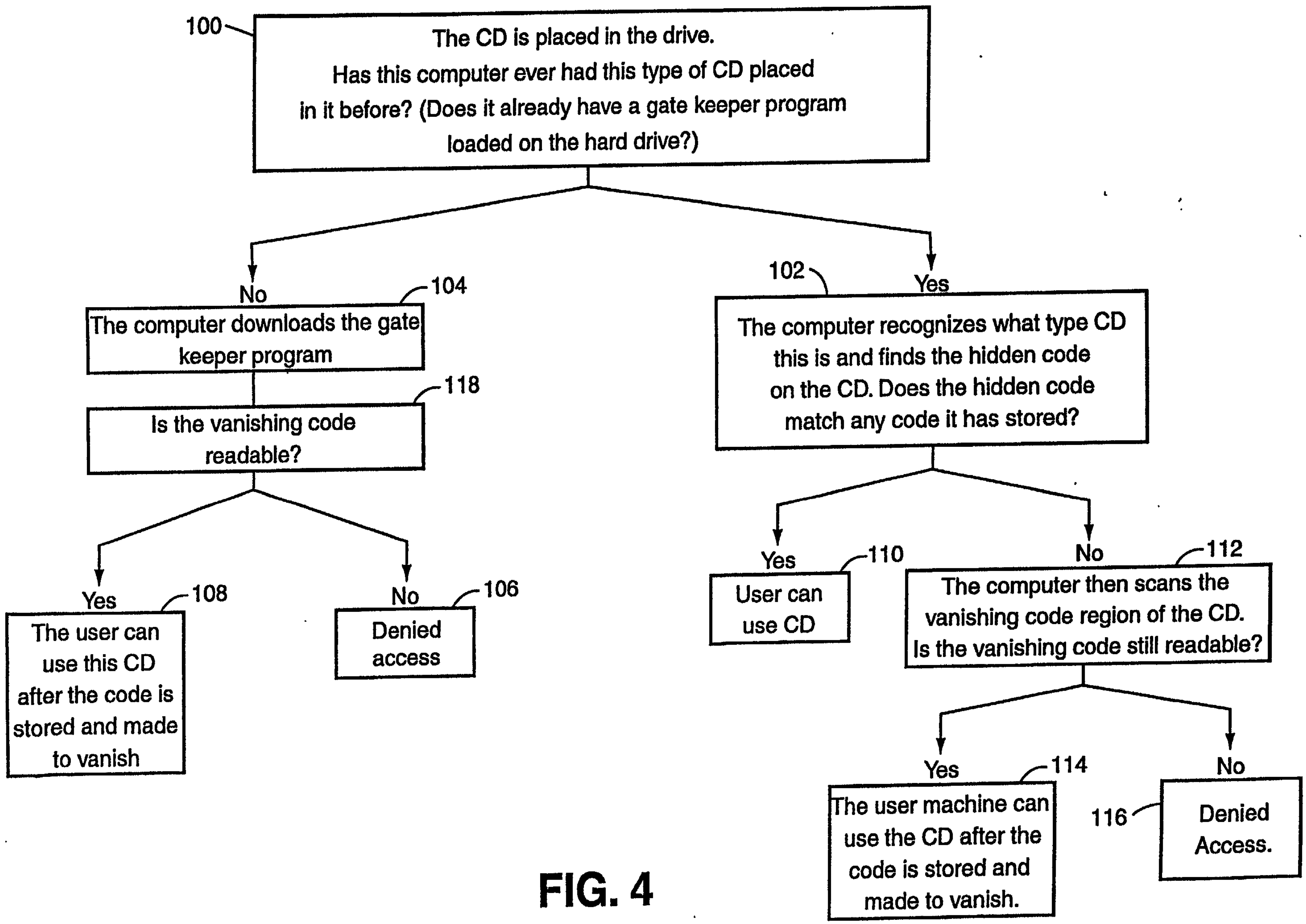


FIG. 3



100
The CD is placed in the drive.
Has this computer ever had this type of CD placed in it before? (Does it already have a gate keeper program loaded on the hard drive?)
No
104
The computer downloads the gate keeper program
118
Is the vanishing code readable?
Yes
108
The user can use this CD after the code is stored and made to vanish
No
106
Denied access
102
Yes
The computer recognizes what type CD this is and finds the hidden code on the CD. Does the hidden code match any code it has stored?
Yes
110
User can use CD
No
112
The computer then scans the vanishing code region of the CD. Is the vanishing code still readable?
Yes
114
The user machine can use the CD after the code is stored and made to vanish.
No
116
Denied Access.

FIG. 4

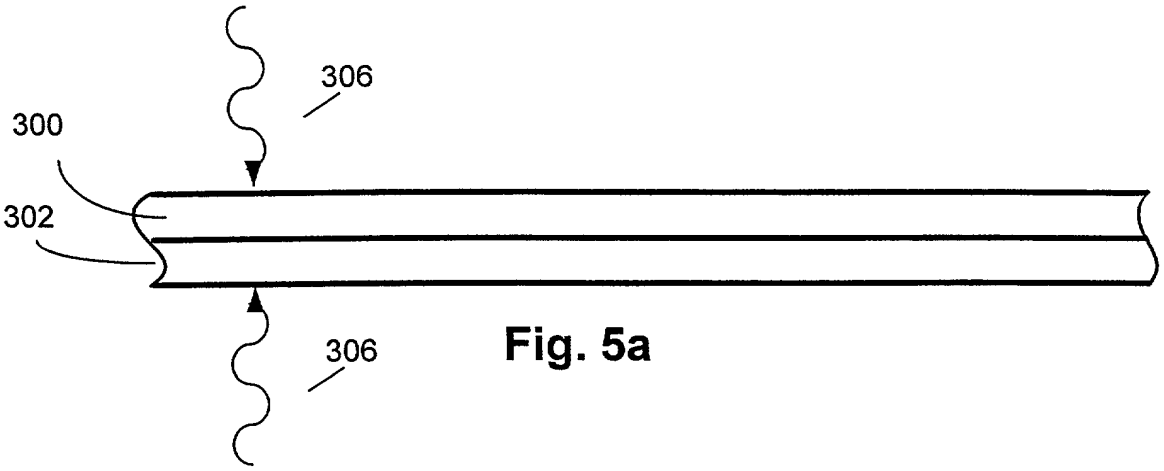


Fig. 5a

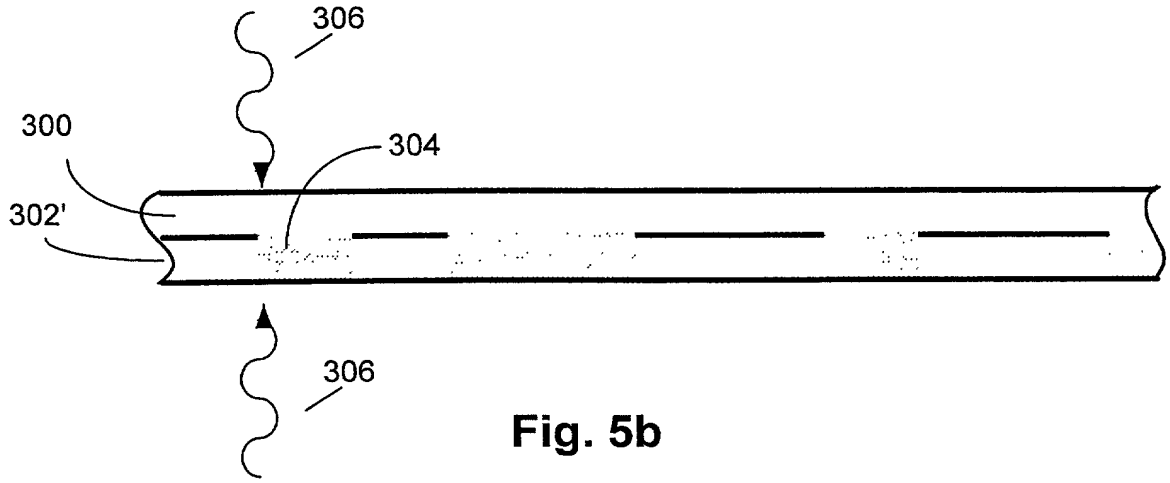


Fig. 5b

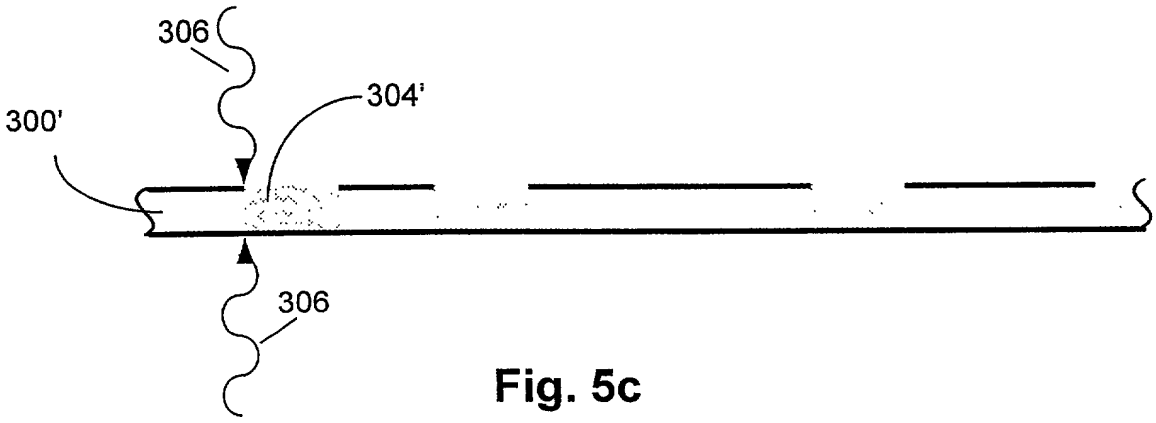


Fig. 5c

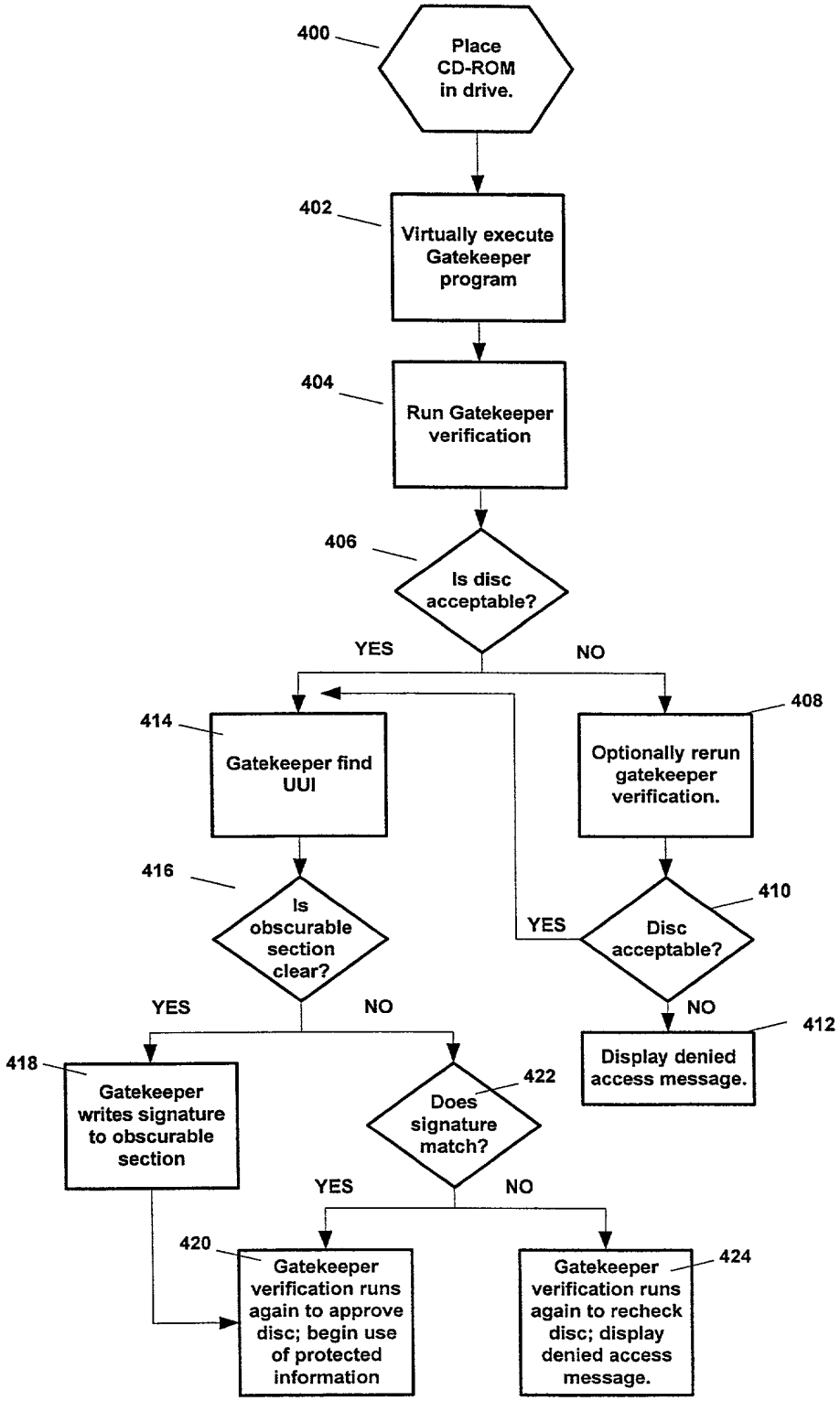

400
Place CD-ROM in drive.
402
Virtually execute Gatekeeper program
404
Run Gatekeeper verification
406
Is disc acceptable?
YES
NO
414
Gatekeeper find UUI
408
Optionally rerun gatekeeper verification.
416
Is obscurable section clear?
410
Disc acceptable?
YES
YES
NO
NO
412
Display denied access message.
418
Gatekeeper writes signature to obscurable section
422
Does signature match?
YES
NO
420
Gatekeeper verification runs again to approve disc; begin use of protected information
424
Gatekeeper verification runs again to recheck disc; display denied access message.

FIG. 6

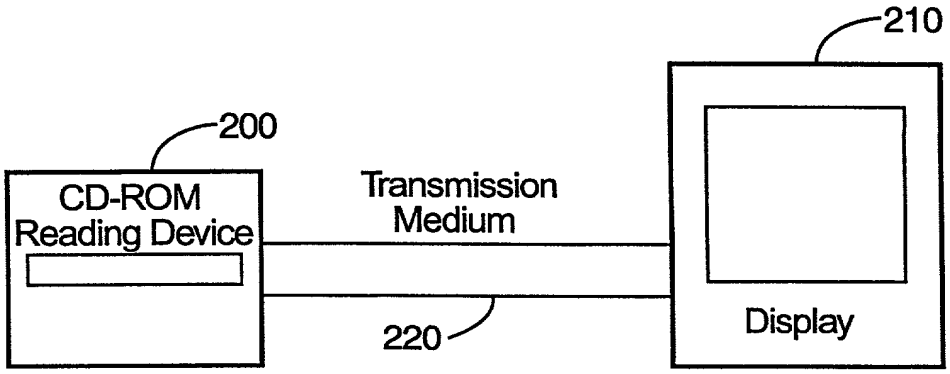

210
200
CD-ROM
Reading Device
Transmission
Medium
220
Display

FIG. 7

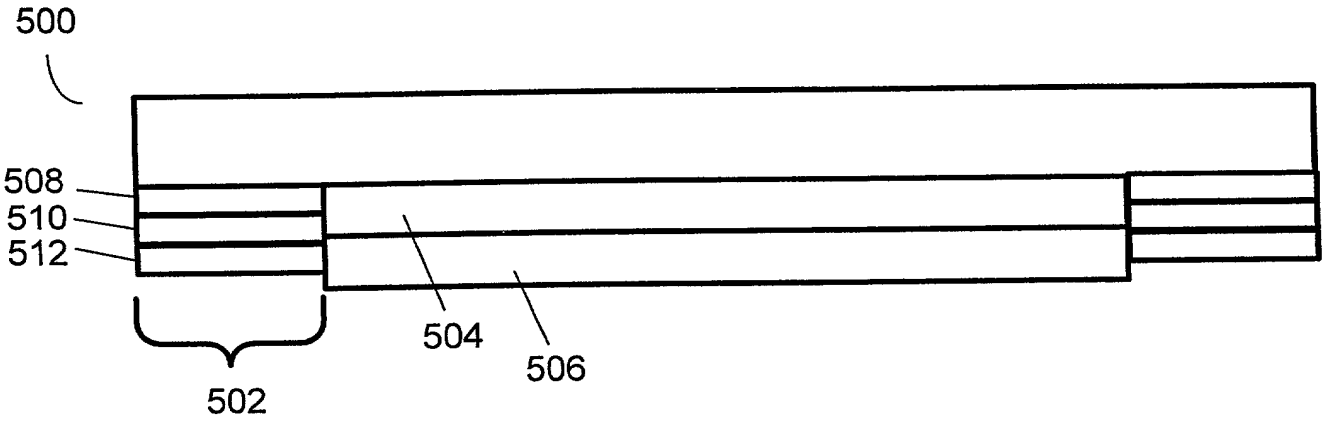


FIG. 8

PATENT
Attorney's Docket No. 206314

COMBINED DECLARATION AND POWER OF ATTORNEY

As below named inventor, I hereby declare that

This declaration is of the following type:
☐ original ☐ design ☐ supplemental
☐ national stage of PCT
☐ divisional ☐ continuation ☒ continuation-in-part

My residence, post office address, and citizenship are as stated below next to my name. I believe I am the original, first, and sole inventor *(if only one name is listed below)* or an original, first, and joint inventor *(if plural names are listed below)* of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND APPARATUS FOR SECURELY ASSOCIATING AN OPTICALLY READABLE MEMORY WITH A USER MACHINE

the specification of which:

☒ is attached hereto.

☐ was filed on as Application No. and was amended on _____ *(if applicable)*.

☐ was filed by Express Mail No. *as Application No. not known yet*, and was amended on _____ *(if applicable)*.

☐ was described and claimed in PCT International Application No. _____ filed on _____ and as amended pursuant to PCT Article 19 on _____ *(if any)*.

I state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above.

I acknowledge the duty to disclose information that is material to the patentability of this application in accordance with 37 C.F.R. § 1.56.

I claim foreign priority benefits under 35 U.S.C. § 119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent, utility model, design registration, or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.

PRIOR FOREIGN PATENT, UTILITY MODEL, AND DESIGN REGISTRATION APPLICATIONS						
COUNTRY	APPLICATION	DATE OF FILING (day, **month**, year)	PRIORITY CLAIMED UNDER 35 U.S.C. § 119			
				YES		NO
				YES		NO
				YES		NO

I claim the benefit pursuant to 35 U.S.C. § 119(e) of the following United States provisional application(s):

PRIOR U.S. PROVISIONAL APPLICATIONS BENEFIT CLAIMED UNDER 35 U.S.C. 119(e)	
APPLICATION NO.	DATE OF FILING (day,**month**,year)

I claim the benefit pursuant to 35 U.S.C. § 120 of any United States application(s) or PCT international application(s) designating the United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose material information as defined in 37 C.F.R. § 1.56 effective between the filing date of the prior application(s) and the national or PCT international filing date of this application.

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL PATENT APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. 120					
U.S. APPLICATIONS			Status *(check one)*		
APPLICATION NO.	U.S. FILING DATE		PATENTED	PENDING	ABANDONED
1. 09/190,511	November 12, 1998			X	
2. 0 /					
3. 0 /					
PCT APPLICATIONS DESIGNATING THE U.S.			Status *(check one)*		
PCT APPLICATION NO.	PCT FILING DATE (day,**month**,year)	U.S. APPLN. NOS. ASSIGNED (if any)	PATENTED	PENDING	ABANDONED
4.					
5.					
6.					

DETAILS OF FOREIGN APPLICATIONS FROM WHICH PRIORITY CLAIMED UNDER 35 U.S.C. §119 FOR ABOVE LISTED U.S./PCT APPLICATIONS				
ABOVE APPLN. NO.	COUNTRY	APPLICATION NO.	DATE OF FILING (day,**month**,year)	DATE OF ISSUE (day,**month**,year)
1.				
2.				
3.				
4.				
5.				
6.				

As a named inventor, I hereby appoint the following attorneys to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

In re Appln. of Gaston
Attorney Docket No. 206314

James B. Muskal, Reg. 22797
Dennis R. Schlemmer, Reg. 24703
Gordon R. Coons, Reg. 20821
John E. Rosenquist, Reg. 26356
John W. Kozak, Reg. 25117
Charles S. Oslakovic, Reg. 27583
Mark E. Phelps, Reg. 28461
H. Michael Hartmann, Reg. 28423
Bruce M. Gagala, Reg. 28844
Charles H. Mottier, Reg. 30874
John Kilyk, Jr., Reg. 30763
Robert F. Green, Reg. 27555
John B. Conklin, Reg. 30369
James D. Zalewa, Reg. 27848
John M. Belz, Reg. 30359
Brett A. Hesterberg, Reg. 31837
Jeffrey A. Wyand, Reg. 29458
Paul J. Korniczky, Reg. 32849
Pamela J. Ruschau, Reg. 34242
Steven P. Petersen, Reg. 32927

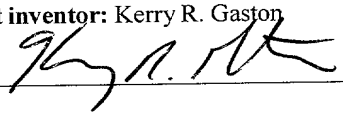
John M. Augustyn, Reg. 33589
Christopher T. Griffith, Reg. 33392
Wesley O. Mueller, Reg. 33976
Jeremy M. Jay, Reg. 33587
Jeffrey B. Burgan, Reg. 35463
Eley O. Thompson, Reg. 36035
Mark Joy, Reg. 35562
Allen E. Hoover, Reg. 37354
David M. Airan, Reg. 38811
Xavier Pillai, Reg. 39799
Y. Kurt Chang, Reg. 41397
Gregory C. Bays, Reg. 40505
Carol Larcher, Reg. 35243
Steven H. Sklar, Reg. 42154
M. Daniel Hefner, Reg. 41826
Thomas A. Belush, Reg. 37090
Kenneth P. Spina, Reg. 43927
Siegmunc Y. Gutman, Reg. 46304
Andrea M. Augustine, Reg. 46526

Andrew J. Heinisch, Reg. 43666
Jeffery J. Makeever, Reg. 37390
Salim A. Hasan, Reg. 38175
Richard A. Wulff, Reg. 42238
Phillip M. Pippenger, Reg. 46055
Jamison E. Lynch, Reg. 41168
Vladan M. Vasiljevic, Reg. 45177
Kathryn M. Lumb, Reg. 46885
Rattan Nath, Reg. 43827
Robert M. Gould, Reg. 43642
Len Smith, Reg. 43139
Kevin L. Wingate, Reg. 38662
Michael N. Spink, Reg. 47107
David J. Schodin, Reg. 41294
Heather R. Kissling, Reg. 45790
Paul L. Ahern, Reg. 17020
Theodore W. Anderson, Reg. 17035
Berton Scott Sheppard, Reg. 20922
Noel I. Smith, Reg. 18698

I further direct that correspondence concerning this application be directed to LEYDIG, VOIT & MAYER, LTD., Two Prudential Plaza, Suite 4900, 180 North Stetson, Chicago, Illinois 60601-6780, Telephone (312) 616-5600.

I declare that all statements made herein of my own knowledge are true, that all statements made on information and belief are believed to be true, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of **sole or first inventor:** Kerry R. Gaston

Inventor's signature 

Date 11/16/00

Country of Citizenship: U.S.A.

Residence: Montgomery, Alabama
(city/state or country)

Post Office Address: ~~2724 West Aberdeen Drive~~ 316 Chrystan CT KRG, Montgomery, AL 36116 36109 KRG
(complete mailing address)

gaston\206314\206314 decpower